

EXHIBIT H

AU Section 324

Service Organizations^{*}

(Supersedes SAS No. 44)

Sources: SAS No. 70; SAS No. 78; SAS No. 88; SAS No. 98.

See section 9324 for interpretations of this section.

Effective for service auditors' reports dated after March 31, 1993, unless otherwise indicated.

Introduction and Applicability

.01 This section provides guidance on the factors an independent auditor should consider when auditing the financial statements of an entity that uses a service organization to process certain transactions. This section also provides guidance for independent auditors who issue reports on the processing of transactions by a service organization for use by other auditors.

.02 For purposes of this section, the following definitions apply.

- *User organization*—The entity that has engaged a service organization and whose financial statements are being audited
- *User auditor*—The auditor who reports on the financial statements of the user organization
- *Service organization*—The entity (or segment of an entity) that provides services to a user organization that are part of the user organization's information system
- *Service auditor*—The auditor who reports on controls of a service organization that may be relevant to a user organization's internal control as it relates to an audit of financial statements
- *Report on controls placed in operation*—A service auditor's report on a service organization's description of its controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, on whether such controls were suitably designed to achieve specified control objectives, and on whether they had been placed in operation as of a specific date
- *Report on controls placed in operation and tests of operating effectiveness*—A service auditor's report on a service organization's description of its controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements,¹ on whether such controls were suitably designed to achieve specified control objectives, on whether they had been placed in operation as of a specific

^{*} Title amended, effective December 1999, by Statement on Auditing Standards No. 88.

¹ In this section, a service organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements will be referred to as a service organization's controls.

date, and on whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified

[Revised, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94.]

.03 The guidance in this section is applicable to the audit of the financial statements of an entity that obtains services from another organization that are part of its information system. A service organization's services are part of an entity's information system if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the entity's financial statements
- The procedures, both automated and manual, by which the entity's transactions are initiated, authorize, recorded, processed, and reported from their occurrence to their inclusion in the financial statements
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the entity's financial statements involved in initiating, recording, processing and reporting the entity's transactions
- How the entity's information system captures other events and conditions that are significant to the financial statements
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures

Service organizations that provide such services include, for example, bank trust departments that invest and service assets for employee benefit plans or for others, mortgage bankers that service mortgages for others, and application service providers that provide packaged software applications and a technology environment that enables customers to process financial and operational transactions. The guidance in this section may also be relevant to situations in which an organization develops, provides, and maintains the software used by client organizations. The provisions of this section are not intended to apply to situations in which the services provided are limited to executing client organization transactions that are specifically authorized by the client, such as the processing of checking account transactions by a bank or the execution of securities transactions by a broker. This section also is not intended to apply to the audit of transactions arising from financial interests in partnerships, corporations, and joint ventures, such as working interests in oil and gas ventures, when proprietary interests are accounted for and reported to interest holders. [As amended, effective December 1999, by Statement on Auditing Standards No. 88, Revised, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 106.]

.04 This section is organized into the following sections.

- a. The user auditor's consideration of the effect of the service organization on the user organization's internal control and the availability of evidence to:
 - Obtain the necessary understanding of the user organization's internal control to assess the risks of material misstatement.

- Assess the risks of material misstatement at the user organization.
- Perform further audit procedures.
- b. Considerations in using a service auditor's report.
- c. Responsibilities of service auditors.

[Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

The User Auditor's Consideration of the Effect of the Service Organization on the User Organization's Internal Control and the Availability of Audit Evidence

.05 The user auditor should consider the discussion in paragraphs .06-.21 when obtaining an understanding of the entity and its environment, including its internal controls and performing the audit of an entity that uses a service organization to process its transactions. [Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

The Effect of Use of a Service Organization on a User Organization's Internal Control

.06 When a user organization uses a service organization, transactions that affect the user organization's financial statements are subjected to controls that are, at least in part, physically and operationally separate from the user organization. The significance of the controls of the service organization to those of the user organization depends on the nature of the services provided by the service organization, primarily the nature and materiality of the transactions it processes for the user organization and the degree of interaction between its activities and those of the user organization. To illustrate how the degree of interaction affects user organization controls, when the user organization initiates transactions and the service organization executes and does the accounting processing of those transactions, there is a high degree of interaction between the activities at the user organization and those at the service organization. In these circumstances, it may be practicable for the user organization to implement effective controls for those transactions. However, when the service organization initiates, executes, and does the accounting processing of the user organization's transactions, there is a lower degree of interaction and it may not be practicable for the user organization to implement effective controls for those transactions. [As amended, effective December 1999, by Statement on Auditing Standards No. 88.]

Planning the Audit

.07 Section 314, *Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement*, states that an auditor should obtain an understanding of each of the five components of the entity's internal control sufficient to assess the risks of material misstatement and to design the nature, timing, and extent of further audit procedures. This understanding may encompass controls placed in operation by the entity and by service organizations whose services are part of the entity's information system. The auditor should use such knowledge to:

- Identify types of potential misstatements.
- Consider factors that affect the risks of material misstatement.

- Design tests of controls, when applicable. Paragraphs .23–.27 of section 318 discuss factors the auditor considers in determining whether to perform tests of controls
- Design substantive tests.

[As amended, effective for service auditor's reports covering descriptions as of or after January 1, 1997, by Statement on Auditing Standards No. 78. As amended, effective December 1999, by Statement on Auditing Standards No. 88. Revised, May 2001, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, March 2006 and May 2007, to reflect conforming changes necessary due to the issuance of Statements on Auditing Standards No. 109 and No. 110.]

[.08] [Paragraph deleted by the issuance of Statement on Auditing Standards No. 88, December 1999.]

.09 Information about the nature of the services provided by a service organization that are part of the user organization's information system and the service organization's controls over those services may be available from a wide variety of sources, such as user manuals, system overviews, technical manuals, the contract between the user organization and the service organization, and reports by service auditors, internal auditors, or regulatory authorities on the service organization's controls. If the services and the service organization's controls over those services are highly standardized, information obtained through the user auditor's prior experience with the service organization may be helpful in assessing the risks of material misstatement. [As amended, effective December 1999, by Statement on Auditing Standards No. 88. Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.10 After considering the available information, the user auditor may conclude that he or she has the means to obtain a sufficient understanding of internal control to assess the risks of material misstatement. If the user auditor concludes that information is not available to obtain a sufficient understanding to assess the risks of material misstatement, he or she may consider contacting the service organization, through the user organization, to obtain specific information or request that a service auditor be engaged to perform procedures that will supply the necessary information, or the user auditor may visit the service organization and perform such procedures. If the user auditor is unable to obtain sufficient audit evidence to achieve his or her audit objectives, the user auditor should qualify his or her opinion or disclaim an opinion on the financial statements because of a scope limitation. [As amended, effective December 1999, by Statement on Auditing Standards No. 88. Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

Assessing Control Risk at the User Organization

.11 The user auditor uses his or her understanding of the internal control to assess control risk for the assertions embodied in the account balances and classes of transactions, including those that are affected by the activities of the service organization. In doing so, the user auditor may identify certain user organization controls that, if effective, would permit the user auditor to assess control risk as low or moderate for particular assertions. Such controls may be applied at either the user organization or the service organization. The user auditor may conclude that it would be efficient to obtain audit evidence about the operating effectiveness of controls to provide a basis for assessing control risk as low or moderate. [Revised, April 2002, to reflect conforming

Service Organizations

267

changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 105. Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.12 A service auditor's report on controls placed in operation at the service organization should be helpful in providing a sufficient understanding to assess the risks of material misstatement of the user organization. Such a report, however, is not intended to provide any evidence of the operating effectiveness of the relevant controls that would allow the user auditor to reduce the assessed level of control risk as low or moderate. Such audit evidence should be derived from one or more of the following:

- a. Tests of the user organization's controls over the activities of the service organization (for example, the user auditor may test the user organization's independent reperformance of selected items processed by a service organization or test the user organization's reconciliation of output reports with source documents)
- b. A service auditor's report on controls placed in operation and tests of operating effectiveness, or a report on the application of agreed-upon procedures that describes relevant tests of controls
- c. Appropriate tests of controls performed by the user auditor at the service organization

[Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 105. Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.13 The user organization may establish effective controls over the service organization's activities that may be tested and that may enable the user auditor to reduce the assessed level of control risk as low or moderate for some or all of the relevant assertions. If a user organization, for example, uses a service organization to process its payroll transactions, the user organization may establish controls over the submission and receipt of payroll information that could prevent or detect material misstatements. The user organization might reperform the service organization's payroll calculations on a test basis. In this situation, the user auditor should obtain a sufficient understanding of the user organization's controls over payroll processing to (1) evaluate the design of such controls and (2) determine whether they have been implemented. The understanding of the user organization's controls over payroll processing would provide a basis for assessing control risk for the assertions related to payroll transactions. [Revised, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.14 The user auditor may find that controls relevant to assessing control risk as low or moderate for particular assertions are applied only at the service organization. If the user auditor plans to assess control risk as low or moderate for those assertions, he or she should evaluate the operating effectiveness of those controls by obtaining a service auditor's report that describes the results of the service auditor's tests of those controls (that is, a report on controls placed in operation and tests of operating effectiveness, or an agreed-upon procedures

report)² or by performing tests of controls at the service organization. If the user auditor decides to use a service auditor's report, the user auditor should consider the extent of the evidence provided by the report about the effectiveness of controls intended to prevent or detect material misstatements in the particular assertions. The user auditor remains responsible for evaluating the evidence presented by the service auditor and for determining its effect on the assessment of control risk at the user organization. [Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.15 The user auditor's assessments of control risk regarding assertions about account balances or classes of transactions are based on the combined evidence provided by the service auditor's report and the user auditor's own procedures. In making these assessments, the user auditor should consider the nature, source, and interrelationships among the evidence, as well as the period covered by the tests of controls. The user auditor uses the assessed levels of control risk, as well as his or her understanding of internal control, in determining the nature, timing, and extent of substantive tests for particular assertions.

.16 The guidance in section 326.06, regarding the auditor's consideration of the sufficiency of audit evidence to support a specific assessed level of control risk is applicable to user auditors considering audit evidence provided by a service auditor's report on controls placed in operation and tests of operating effectiveness. Because the report may be intended to satisfy the needs of several different user auditors, a user auditor should determine whether the specific tests of controls and results in the service auditor's report are relevant to assertions that are significant in the user organization's financial statements. For those tests of controls and results that are relevant, a user auditor should consider whether the nature, timing, and extent of such tests of controls and results provide appropriate evidence about the effectiveness of the controls to support the user auditor's assessed level of control risk. In evaluating these factors, user auditors should also keep in mind that, for certain assertions, the shorter the period covered by a specific test and the longer the time elapsed since the performance of the test, the less support for control risk reduction the test may provide. [Revised, May 2001, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statements on Auditing Standards No. 105 and No. 106.]

Audit Evidence From Substantive Audit Procedures Performed by Service Auditors

.17 Service auditors may be engaged to perform procedures that are substantive in nature for the benefit of user auditors. Such engagements may involve the performance, by the service auditor, of procedures agreed upon by the user organization and its auditor and by the service organization and its auditor. In addition, there may be requirements imposed by governmental authorities or through contractual arrangements whereby service auditors perform designated procedures that are substantive in nature. The results of the application of the required procedures to balances and transactions processed by the service

² See AT section 201, *Agreed-Upon Procedures Engagements*, for guidance on performing and reporting on agreed-upon procedures engagements. [Footnote added, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 10.]

organization may be used by user auditors as part of the evidence necessary to support their opinions.

Considerations in Using a Service Auditor's Report

.18 In considering whether the service auditor's report is satisfactory for his or her purposes, the user auditor should make inquiries concerning the service auditor's professional reputation. Appropriate sources of information concerning the professional reputation of the service auditor are discussed in section 543, *Part of Audit Performed by Other Independent Auditors*, paragraph .10a.

.19 In considering whether the service auditor's report is sufficient to meet his or her objectives, the user auditor should give consideration to the guidance in section 543.12. If the user auditor believes that the service auditor's report may not be sufficient to meet his or her objectives, the user auditor may supplement his or her understanding of the service auditor's procedures and conclusions by discussing with the service auditor the scope and results of the service auditor's work. Also, if the user auditor believes it is necessary, he or she may contact the service organization, through the user organization, to request that the service auditor perform agreed-upon procedures at the service organization, or the user auditor may perform such procedures.

.20 When assessing a service organization's controls and how they interact with a user organization's controls, the user auditor may become aware of the existence of significant deficiencies or material weaknesses in internal control. In such circumstances, the user auditor should consider the guidance provided in section 325, *Communicating Internal Control Related Matters Identified in an Audit*. [Revised, May 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 112.]

.21 The user auditor should not make reference to the report of the service auditor as a basis, in part, for his or her own opinion on the user organization's financial statements. The service auditor's report is used in the audit, but the service auditor is not responsible for examining any portion of the financial statements as of any specific date or for any specified period. Thus, there cannot be a division of responsibility for the audit of the financial statements.

Responsibilities of Service Auditors

.22 The service auditor is responsible for the representations in his or her report and for exercising due care in the application of procedures that support those representations. Although a service auditor's engagement differs from an audit of financial statements conducted in accordance with generally accepted auditing standards, it should be performed in accordance with the general standards and with the relevant fieldwork and reporting standards. Although the service auditor should be independent from the service organization, it is not necessary for the service auditor to be independent from each user organization.

.23 As a result of procedures performed at the service organization, the service auditor may become aware of illegal acts, fraud, or uncorrected errors attributable to the service organization's management or employees that may affect one or more user organizations. The terms *errors*, *fraud*, and *illegal acts* are discussed in section 312, *Audit Risk and Materiality in Conducting an Audit*, and section 317, *Illegal Acts by Clients*; the discussions therein are relevant to this section. When the service auditor becomes aware of such matters, he or she should determine from the appropriate level of management of the service organization whether this information has been communicated appropriately

to affected user organizations, unless those matters are clearly inconsequential. If the management of the service organization has not communicated the information to affected user organizations and is unwilling to do so, the service auditor should inform those charged with governance of the service organization. If those charged with governance do not respond appropriately to the service auditor's communication, the service auditor should consider whether to resign from the engagement. The service auditor may wish to consult with his or her attorney in making this decision. [Revised, April 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 114.]

.24 The type of engagement to be performed and the related report to be prepared should be established by the service organization. However, when circumstances permit, discussions between the service organization and the user organizations are advisable to determine the type of report that will be most suitable for the user organizations' needs. This section provides guidance on the two types of reports that may be issued:

- a. *Reports on controls placed in operation*—A service auditor's report on a service organization's description of the controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, on whether such controls were suitably designed to achieve specified control objectives, and on whether they had been placed in operation as of a specific date. Such reports may be useful in providing a user auditor with an understanding of the controls necessary to assess the risks of material misstatement and to design effective tests of controls and substantive tests at the user organization, but they are not intended to provide the user auditor with a basis for reducing his or her assessments of control risk as low or moderate.
- b. *Reports on controls placed in operation and tests of operating effectiveness*—A service auditor's report on a service organization's description of the controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, on whether such controls were suitably designed to achieve specified control objectives, on whether they had been placed in operation as of a specific date, and on whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. Such reports may be useful in providing the user auditor with an understanding of the controls necessary to plan the audit and may also provide the user auditor with a basis for reducing his or her assessments of control risk as low or moderate.

[Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

Reports on Controls Placed in Operation

.25 The information necessary for a report on controls placed in operation ordinarily is obtained through discussions with appropriate service organization personnel and through reference to various forms of documentation, such as system flowcharts and narratives.

.26 After obtaining a description of the relevant controls, the service auditor should determine whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the service organization's controls that may be relevant to a user organization's internal control. The description should contain a discussion of the features of the service

Service Organizations

271

organization's controls that would have an effect on a user organization's internal control. Such features are relevant when they directly affect the service provided to the user organization. They may include controls within the control environment, risk assessment, control activities, information and communication, and monitoring components of internal control. The control environment may include hiring practices and key areas of authority and responsibility. Risk assessment may include the identification of risks associated with processing specific transactions. Control activities may include policies and procedures over the modification of computer programs and are ordinarily designed to meet specific control objectives. The specific control objectives of the service organization should be set forth in the service organization's description of controls. Information and communication may include ways in which user transactions are initiated and processed. Monitoring may include the involvement of internal auditors. [As amended, effective for service auditor's reports covering descriptions as of or after January 1, 1997, by Statement on Auditing Standards No. 78.]

.27 Evidence of whether controls have been placed in operation is ordinarily obtained through previous experience with the service organization and through procedures such as inquiry of appropriate management, supervisory, and staff personnel; inspection of service organization documents and records; and observation of service organization activities and operations. For the type of report described in paragraph .24a, these procedures need not be supplemented by tests of the operating effectiveness of the service organization's controls.

.28 Although a service auditor's report on controls placed in operation is as of a specified date, the service auditor should inquire about changes in the service organization's controls that may have occurred before the beginning of fieldwork. If the service auditor believes that the changes would be considered significant by user organizations and their auditors, those changes should be included in the description of the service organization's controls. If the service auditor concludes that the changes would be considered significant by user organization's and their auditors and the changes are not included in the description of the service organization's controls, the service auditor should describe the changes in his or her report. Such changes might include:

- Procedural changes made to accommodate provisions of a new FASB Statement of Financial Accounting Standards.
- Major changes in an application to permit on-line processing.
- Procedural changes to eliminate previously identified deficiencies.

Changes that occurred more than twelve months before the date being reported on normally would not be considered significant, because they generally would not affect user auditors' considerations.

.29 A service auditor's report expressing an opinion on a description of controls placed in operation at a service organization should contain:

- a. A specific reference to the applications, services, products, or other aspects of the service organization covered.
- b. A description of the scope and nature of the service auditor's procedures.
- c. Identification of the party specifying the control objectives.
- d. An indication that the purpose of the service auditor's engagement was to obtain reasonable assurance about whether (1) the service organization's description presents fairly, in all material respects, the aspects of the service organization's controls that may be relevant to a

user organization's internal control as it relates to an audit of financial statements, (2) the controls were suitably designed to achieve specified control objectives, and (3) such controls had been placed in operation as of a specific date.

- e. A disclaimer of opinion on the operating effectiveness of the controls.
- f. The service auditor's opinion on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date and whether, in the service auditor's opinion, the controls were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those controls were complied with satisfactorily.
- g. A statement of the inherent limitations of the potential effectiveness of controls at the service organization and of the risk of projecting to future periods any evaluation of the description.
- h. Identification of the parties for whom the report is intended.

.30 If the service auditor believes that the description is inaccurate or insufficiently complete for user auditors, the service auditor's report should so state and should contain sufficient detail to provide user auditors with an appropriate understanding.

.31 It may become evident to the service auditor, when considering the service organization's description of controls placed in operation, that the system was designed with the assumption that certain controls would be implemented by the user organization. If the service auditor is aware of the need for such complementary user organization controls, these should be delineated in the description of controls. If the application of controls by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the controls contemplated in the design of the Service Organization's controls" following the words "complied with satisfactorily" in the scope and opinion paragraphs.

.32 The service auditor should consider conditions that come to his or her attention that, in the service auditor's judgment, represent significant deficiencies in the design or operation of the service organization's controls that preclude the service auditor from obtaining reasonable assurance that specified control objectives would be achieved. The service auditor should also consider whether any other information, irrespective of specified control objectives, has come to his or her attention that causes him or her to conclude (a) that design deficiencies exist that could adversely affect the ability to initiate, authorize, record, process, or report financial data to user organizations without error, and (b) that user organizations would not generally be expected to have controls in place to mitigate such design deficiencies. [Revised, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 106.]

.33 The description of controls and control objectives required for these reports may be prepared by the service organization. If the service auditor prepares the description of controls and control objectives, the representations in the description remain the responsibility of the service organization.

.34 For the service auditor to express an opinion on whether the controls were suitably designed to achieve the specified control objectives, it is necessary that:

Service Organizations

273

- a. The service organization identify and appropriately describe such control objectives and the relevant controls.
- b. The service auditor consider the linkage of the controls to the stated control objectives.
- c. The service auditor obtain sufficient appropriate audit evidence to reach an opinion.

.35 The control objectives may be designated by the service organization or by outside parties such as regulatory authorities, a user group, or others. When the control objectives are not established by outside parties, the service auditor should be satisfied that the control objectives, as set forth by the service organization, are reasonable in the circumstances and consistent with the service organization's contractual obligations.

.36 The service auditor's report should state whether the controls were suitably designed to achieve the specified control objectives. The report should not state whether they were suitably designed to achieve objectives beyond the specifically identified control objectives.

.37 The service auditor's opinion on whether the controls were suitably designed to achieve the specified control objectives is not intended to provide evidence of operating effectiveness or to provide the user auditor with a basis for concluding that control risk may be assessed as low or moderate. [Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.38 The following is a sample report on controls placed in operation at a service organization. The report should have, as an attachment, a description of the service organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements. This report is illustrative only and should be modified as appropriate to suit the circumstances of individual engagements.

To XYZ Service Organization:

We have examined the accompanying description of controls related to the __ application of XYZ Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily,³ and (3) such controls had been placed in operation as of _____. The control objectives were specified by _____. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of XYZ Service Organization's controls, individually or in the aggregate.

³ If the application of controls by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the controls contemplated in the design of XYZ Service Organization's controls" following the words "complied with satisfactorily" in the scope and opinion paragraphs. [Footnote renumbered, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 10.]

The Standards of Field Work

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had been placed in operation as of _____. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

The description of controls at XYZ Service Organization is as of _____ and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the Service Organization is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers _____.

.39 If the service auditor concludes that the description is inaccurate or insufficiently complete for user auditors, the service auditor should so state in an explanatory paragraph preceding the opinion paragraph. An example of such an explanatory paragraph follows:

The accompanying description states that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and inspections of activities, we determined that such procedures are employed in Applications A and B but are not required to access the system in Applications C and D.

In addition, the first sentence of the opinion paragraph would be modified to read as follows:

In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had been placed in operation as of _____.

.40 If, after applying the criteria in paragraph .32, the service auditor concludes that there are significant deficiencies in the design or operation of the service organization's controls, the service auditor should report those conditions in an explanatory paragraph preceding the opinion paragraph. An example of an explanatory paragraph describing a significant deficiency in the design or operation of the service organization's controls follows:

As discussed in the accompanying description, from time to time the Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.

In addition, the second sentence of the opinion paragraph would be modified to read as follows:

Also in our opinion, except for the deficiency referred to in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

Reports on Controls Placed in Operation and Tests of Operating Effectiveness

Paragraphs .41-.56 repeat some of the information contained in paragraphs .25-.40 to provide readers with a comprehensive, stand-alone presentation of the relevant considerations for each type of report.

.41 The information necessary for a report on controls placed in operation and tests of operating effectiveness ordinarily is obtained through discussions with appropriate service organization personnel, through reference to various forms of documentation, such as system flowcharts and narratives, and through the performance of tests of controls. Evidence of whether controls have been placed in operation is ordinarily obtained through previous experience with the service organization and through procedures such as inquiry of appropriate management, supervisory, and staff personnel; inspection of service organization documents and records; and observation of service organization activities and operations. The service auditor applies tests of controls to determine whether specific controls are operating with sufficient effectiveness to achieve specified control objectives. Section 350, *Audit Sampling*, as amended, provides guidance on the application and evaluation of audit sampling in performing tests of controls.

.42 After obtaining a description of the relevant controls, the service auditor should determine whether the description provides sufficient information for user auditors to obtain an understanding of those aspects of the service organization's controls that may be relevant to a user organization's internal control. The description should contain a discussion of the features of the service organization's controls that would have an effect on a user organization's internal control. Such features are relevant when they directly affect the service provided to the user organization. They may include controls within the control environment, risk assessment, control activities, information and communication, and monitoring components of internal control. The control environment may include hiring practices and key areas of authority and responsibility. Risk assessment may include the identification of risks associated with processing specific transactions. Control activities may include policies and procedures over the modification of computer programs and are ordinarily designed to meet specific control objectives. The specific control objectives of the service organization should be set forth in the service organization's description of controls. Information and communication may include ways in which user transactions are initiated and processed. Monitoring may include the involvement of internal auditors. [As amended, effective for service auditor's reports covering descriptions as of or after January 1, 1997, by Statement on Auditing Standards No. 78.]

.43 The service auditor should inquire about changes in the service organization's controls that may have occurred before the beginning of fieldwork. If the service auditor believes the changes would be considered significant by user organizations and their auditors, those changes should be included in the description of the service organization's controls. If the service auditor concludes that the changes would be considered significant by user organizations and their auditors and the changes are not included in the description of the service organization's controls, the service auditor should describe the changes in his or her report. Such changes might include:

- Procedural changes made to accommodate provisions of a new FASB Statement of Financial Accounting Standards.
- Major changes in an application to permit on-line processing.

- Procedural changes to eliminate previously identified deficiencies.

Changes that occurred more than twelve months before the date being reported on normally would not be considered significant, because they generally would not affect user auditors' considerations.

.44 A service auditor's report expressing an opinion on a description of controls placed in operation at a service organization and tests of operating effectiveness should contain:

- a. A specific reference to the applications, services, products, or other aspects of the service organization covered.
- b. A description of the scope and nature of the service auditor's procedures.
- c. Identification of the party specifying the control objectives.
- d. An indication that the purpose of the service auditor's engagement was to obtain reasonable assurance about whether (1) the service organization's description presents fairly, in all material respects, the aspects of the service organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls were suitably designed to achieve specified control objectives, and (3) such controls had been placed in operation as of a specific date.
- e. The service auditor's opinion on whether the description presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date and whether, in the service auditor's opinion, the controls were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if those controls were complied with satisfactorily.
- f. A reference to a description of tests of specific service organization controls designed to obtain evidence about the operating effectiveness of those controls in achieving specified control objectives. The description should include the controls that were tested, the control objectives the controls were intended to achieve, the tests applied, and the results of the tests. The description should include an indication of the nature, timing, and extent of the tests, as well as sufficient detail to enable user auditors to determine the effect of such tests on user auditors' assessments of control risk. To the extent that the service auditor identified causative factors for exceptions, determined the current status of corrective actions, or obtained other relevant qualitative information about exceptions noted, such information should be provided.
- g. A statement of the period covered by the service auditor's report on the operating effectiveness of the specific controls tested.
- h. The service auditor's opinion on whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.
- i. When all of the control objectives listed in the description of controls placed in operation are not covered by tests of operating effectiveness, a statement that the service auditor does not express an opinion on control objectives not listed in the description of tests performed at the service organization.
- j. A statement that the relative effectiveness and significance of specific service organization controls and their effect on assessments of control

Service Organizations

277

risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations.

- k. A statement that the service auditor has performed no procedures to evaluate the effectiveness of controls at individual user organizations.
- l. A statement of the inherent limitations of the potential effectiveness of controls at the service organization and of the risk of projecting to the future any evaluation of the description or any conclusions about the effectiveness of controls in achieving control objectives.
- m. Identification of the parties for whom the report is intended.

.45 If the service auditor believes that the description is inaccurate or insufficiently complete for user auditors, the service auditor's report should so state and should contain sufficient detail to provide user auditors with an appropriate understanding.

.46 It may become evident to the service auditor, when considering the service organization's description of controls placed in operation, that the system was designed with the assumption that certain controls would be implemented by the user organization. If the service auditor is aware of the need for such complementary user organization controls, these should be delineated in the description of controls. If the application of controls by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the controls contemplated in the design of the Service Organization's controls" following the words "complied with satisfactorily" in the scope and opinion paragraphs. Similarly, if the operating effectiveness of controls at the service organization is dependent on the application of controls at user organizations, this should be delineated in the description of tests performed.

.47 The service auditor should consider conditions that come to his or her attention that, in the service auditor's judgment, represent significant deficiencies in the design or operation of the service organization's controls that preclude the service auditor from obtaining reasonable assurance that specified control objectives would be achieved. The service auditor should also consider whether any other information, irrespective of specified control objectives, has come to his or her attention that causes him or her to conclude (a) that design deficiencies exist that could adversely affect the ability to initiate, authorize, record, process, or report financial data to user organizations without error, and (b) that user organizations would not generally be expected to have controls in place to mitigate such design deficiencies. [Revised, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 94. Revised, March 2006, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 106.]

.48 The description of controls and control objectives required for these reports may be prepared by the service organization. If the service auditor prepares the description of controls and control objectives, the representations in the description remain the responsibility of the service organization.

.49 For the service auditor to express an opinion on whether the controls were suitably designed to achieve the specified control objectives, it is necessary that:

- a. The service organization identify and appropriately describe such control objectives and the relevant controls.
- b. The service auditor consider the linkage of the controls to the stated control objectives.
- c. The service auditor obtain sufficient appropriate audit evidence to reach an opinion.

.50 The control objectives may be designated by the service organization or by outside parties such as regulatory authorities, a user group, or others. When the control objectives are not established by outside parties, the service auditor should be satisfied that the control objectives, as set forth by the service organization, are reasonable in the circumstances and consistent with the service organization's contractual obligations.

.51 The service auditor's report should state whether the controls were suitably designed to achieve the specified control objectives. The report should not state whether they were suitably designed to achieve objectives beyond the specifically identified control objectives.

.52 The service auditor's opinion on whether the controls were suitably designed to achieve the specified control objectives is not intended to provide evidence of operating effectiveness or to provide the user auditor with a basis for concluding that control risk may be assessed as low or moderate. Evidence that may enable the user auditor to conclude that control risk may be assessed as low or moderate may be obtained from the results of specific tests of operating effectiveness. [Revised, May 2007, to reflect conforming changes necessary due to the issuance of Statement on Auditing Standards No. 109.]

.53 The management of the service organization specifies whether all or selected applications and control objectives will be covered by the tests of operating effectiveness. The service auditor determines which controls are, in his or her judgment, necessary to achieve the control objectives specified by management. The service auditor then determines the nature, timing, and extent of the tests of controls needed to evaluate operating effectiveness. Testing should be applied to controls in effect throughout the period covered by the report. To be useful to user auditors, the report should ordinarily cover a minimum reporting period of six months.

.54 The following is a sample report on controls placed in operation at a service organization and tests of operating effectiveness. It should be assumed that the report has two attachments: (a) a description of the service organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements and (b) a description of controls for which tests of operating effectiveness were performed, the control objectives the controls were intended to achieve, the tests applied, and the results of those tests. This report is illustrative only and should be modified as appropriate to suit the circumstances of individual engagements.

To XYZ Service Organization:

We have examined the accompanying description of controls related to the ____ application of XYZ Service Organization. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of XYZ Service Organization's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily,⁴ and (3) such controls had been placed in operation as of _____. The control objectives

⁴ If the application of controls by user organizations is necessary to achieve the stated control objectives, the service auditor's report should be modified to include the phrase "and user organizations applied the controls contemplated in the design of XYZ Service Organization's controls" following the words "complied with satisfactorily" in the scope and opinion paragraphs. [Footnote renumbered, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 10.]

Service Organizations

279

were specified by _____. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had been placed in operation as of _____. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Schedule X, to obtain evidence about their effectiveness in meeting the control objectives, described in Schedule X, during the period from _____ to _____. The specific controls and the nature, timing, extent, and results of the tests are listed in Schedule X. This information has been provided to user organizations of XYZ Service Organization and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations. In our opinion the controls that were tested, as described in Schedule X, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Schedule X were achieved during the period from _____ to _____. [However, the scope of our engagement did not include tests to determine whether control objectives not listed in Schedule X were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Schedule X.]⁵

The relative effectiveness and significance of specific controls at XYZ Service Organization and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at XYZ Service Organization is as of _____, and information about tests of the operating effectiveness of specific controls covers the period from _____ to _____. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the Service Organization is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report is intended solely for use by the management of XYZ Service Organization, its customers, and the independent auditors of its customers.

.55 If the service auditor concludes that the description is inaccurate or insufficiently complete for user auditors, the service auditor should so state in an explanatory paragraph preceding the opinion paragraph. An example of such an explanatory paragraph follows:

⁵ This sentence should be added when all of the control objectives listed in the description of controls placed in operation are not covered by the tests of operating effectiveness. This sentence would be omitted when all of the control objectives listed in the description of controls placed in operation are included in the tests of operating effectiveness. [Footnote renumbered, April 2002, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 10.]

The accompanying description states that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and inspection of activities, we determined that such procedures are employed in Applications A and B but are not required to access the system in Applications C and D.

In addition, the first sentence of the opinion paragraph would be modified to read as follows:

In our opinion, except for the matter referred to in the preceding paragraph, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of XYZ Service Organization's controls that had been placed in operation as of ____.

.56 If, after applying the criteria in paragraph .47, the service auditor concludes that there are significant deficiencies in the design or operation of the service organization's controls, the service auditor should report those conditions in an explanatory paragraph preceding the opinion paragraph. An example of an explanatory paragraph describing a significant deficiency in the design or operation of the service organization's controls follows:

As discussed in the accompanying description, from time to time the Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes, and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.

In addition, the second sentence of the opinion paragraph would be modified to read as follows:

Also in our opinion, except for the deficiency referred to in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance that the related control objectives would be achieved if the described controls were complied with satisfactorily.

Responsibilities of Service Organizations and Service Auditors With Respect to Subsequent Events

.57 Changes in a service organization's controls that could affect user organizations' information systems may occur subsequent to the period covered by the service auditor's report but before the date of the service auditor's report. These occurrences are referred to as subsequent events. A service auditor should consider information about two types of subsequent events that come to his or her attention. [Paragraph added, effective for reports issued on or after January 1, 2003, by Statement on Auditing Standards No. 98.]

.58 The first type consists of events that provide additional information about conditions that existed during the period covered by the service auditor's report. This information should be used by the service auditor in determining whether controls at the service organization that could affect user organizations' information systems were placed in operation, suitably designed, and, if applicable, operating effectively during the period covered by the engagement. [Paragraph added, effective for reports issued on or after January 1, 2003, by Statement on Auditing Standards No. 98.]

.59 The second type consists of those events that provide information about conditions that arose subsequent to the period covered by the service auditor's

report that are of such a nature and significance that their disclosure is necessary to prevent users from being misled. This type of information ordinarily will not affect the service auditor's report if the information is adequately disclosed by management in a section of the report containing "Other Information Provided by the Service Organization." If this information is not disclosed by the service organization, the service auditor should disclose it in a section of the report containing "Other Information Provided by the Service Auditor" and/or in the service auditor's report. [Paragraph added, effective for reports issued on or after January 1, 2003, by Statement on Auditing Standards No. 98.]

.60 Although a service auditor has no responsibility to detect subsequent events, the service auditor should inquire of management as to whether it is aware of any subsequent events through the date of the service auditor's report that would have a significant effect on user organizations. In addition, a service auditor should obtain a representation from management regarding subsequent events. [Paragraph added, effective for reports issued on or after January 1, 2003, by Statement on Auditing Standards No. 98.]

Written Representations of the Service Organization's Management

.61 Regardless of the type of report issued, the service auditor should obtain written representations from the service organization's management that:

- Acknowledge management's responsibility for establishing and maintaining appropriate controls relating to the processing of transactions for user organizations.
- Acknowledge the appropriateness of the specified control objectives.
- State that the description of controls presents fairly, in all material respects, the aspects of the service organization's controls that may be relevant to a user organization's internal control.
- State that the controls, as described, had been placed in operation as of a specific date.
- State that management believes its controls were suitably designed to achieve the specified control objectives.
- State that management has disclosed to the service auditor any significant changes in controls that have occurred since the service organization's last examination.
- State that management has disclosed to the service auditor any illegal acts, fraud, or uncorrected errors attributable to the service organization's management or employees that may affect one or more user organizations.
- State that management has disclosed to the service auditor all design deficiencies in controls of which it is aware, including those for which management believes the cost of corrective action may exceed the benefits.
- State that management has disclosed to the service auditor any subsequent events that would have a significant effect on user organizations.

If the scope of the work includes tests of operating effectiveness, the service auditor should obtain a written representation from the service organization's management stating that management has disclosed to the service auditor all instances, of which it is aware, when controls have not operated with sufficient effectiveness to achieve the specified control objectives. [Paragraph renumbered

and amended, effective for reports issued on or after January 1, 2003, by Statement on Auditing Standards No. 98.]

Reporting on Substantive Procedures

.62 The service auditor may be requested to apply substantive procedures to user transactions or assets at the service organization. In such circumstances, the service auditor may make specific reference in his or her report to having carried out the designated procedures or may provide a separate report in accordance with AT section 201, *Agreed-Upon Procedures Engagements*. Either form of reporting should include a description of the nature, timing, extent, and results of the procedures in sufficient detail to be useful to user auditors in deciding whether to use the results as evidence to support their opinions. [Revised, January 2001, to reflect conforming changes necessary due to the issuance of Statement on Standards for Attestation Engagements No. 10. Paragraph renumbered by the issuance of Statement on Auditing Standards No. 98, September 2002.]

Effective Date

.63 This section is effective for service auditors' reports dated after March 31, 1993. Earlier application of this section is encouraged. [Paragraph renumbered by the issuance of Statement on Auditing Standards No. 98, September 2002.]
